Ransomware 2.0: del cifrado de datos a la amenaza de desvelar información confidencial

Los cibercriminales generalizan una táctica de doble extorsión a las compañías víctimas de sus ataques.

Los ataques de ransomware se han sofisticado. Desde el tristémente famoso **Wannacry** de 2017, los cibercriminales han desarrollado nuevas tácticas de amenaza a las empresas. Este año se han generalizado los ataques en los que se realiza una **doble extorsión**. Las organizaciones criminales no sólo cifran los datos de las empresas víctimas, sino que amenazan con publicar información confidencial si no se avienen a pagar un rescate.

Cuando los ciberdelicuentes rompen la seguridad de una compañia, rastrean sus sistemas en busca de información confidencial. Una vez localizada, realizan el cifrado de los datos y extorsionan a las empresas amenazando con la filtración de estos datos y extorsionan a las empresas amenazando con la filtración de estos datos sensibles.

Hay portales en los que se puede seguir la cuenta atrás de las compañias amenazadas

Hay portales en los que se puede ver qué compañias han sido vulveradas y se muestra la cuenta atrás para desvelar esos datos jugosos a los que han accedido los cibercriminales, explica **Daniel Creus, investigador de seguridad del Global Rsearch & Analyst Team de Kaspersky.**

La publicación online de datos confidenciales supone una nueva amenaza porque, además del riesgo reputacional para las empresas víctimas, **expone a las organizaciones a demandas** si los datos publicados violan, por ejemplo, la regulación de protección de privacidad.

Para demostrar que su amenaza es veraz, publican una pequeña muestra de datos en la dark web, asegura la compañia de ciberseguridad **Check Point**, que pronostica que este ipo de *ransomware* segurá siendo una de las grandes amenazas en 2021.

Según sus datos, en el tercer trimestre de este año se ha incrementado la media de ataques diarios de ransomware un 50% respecto al primer semestre.

Recientemente, Endesa sufrió un ciberataque de *ransomware* que afectó al correcto funcionamiento de su servicio ni a los datops de sus empleados o clientes.

ESPECIALIZACIÓN

Creus explica que las **organizaciones cibercriminaes cada vez están más especializadas**. Hay grupos que se dedican a escanear Internet en busca de puntos vulnerables. Luego hacen un cibrado para detectar qué compañias que pueden tener datos más jugosos y venden esta información a otros cibercriminales, que son los que lanzan el ataque con códigos maliciosos que han desarrollado otros ciberdelicuentes, dice.

Els proyecto de descifrado de Europol ha evitado rescates por valor de 600 millones de dólares

Las familias de *ramsomware* que practican los métodos de extorsión llevan nombres como Ragnar Locker, Egregor o Maze. Esta última se ha convertido en una de las más conocidas durante este año, explican en Kaspersky. Incluso se tejen alianzas entre ellos. Este verano, Ragnar Locker declaró que se había unido al grupo Maze para colaborar y compartir información robada.

Incibe(el Instituto Nacional de Ciberseguridad) **desaconseja el pago del rescates,** ya que no existe garantia de recuperar la información y fomenta el lucro de los ciberdelicuentes.

En el caso del *ransomware* tradicional, Incibe aconseja a las compañias afectadas que comprueben si existe una solución de descifrado en el proyecto avalado por la Europol denominado No More Ransom. La iniciativa, en la que participan tambie¡én la Policia Nacional Holandesa y las compañías de ciberseguridad McAfee y Kaspersky, ha cumplido este año su cuarto aniversario. Desde su fundación, ha ayudado a más de cuatro millones de víctimas y ha descifrado 140 familias de *ransomware*. De esta manera, dicen, han evitado rescates por valor de 600 millones de dólares.

Fuente: Expansion